2015

Lattice Polytopes in Coding Theory

Ivan Soprunov
Cleveland State University, i.soprunov@csuohio.edu

J. Algebra Comb. Discrete Appl.
2(2) • 85-94
Received: 31 October 2014; Accepted: 21 February 2015
DOI 10.13069/jacodesmath.75353

Journal of Algebra Combinatorics Discrete Structures and Applications

Lattice polytopes in coding theory

Research Article

Ivan Soprunov*

Department of Mathematics, Cleveland State University, Cleveland, OH USA

Abstract: In this paper we discuss combinatorial questions about lattice polytopes motivated by recent results on minimum distance estimation for toric codes. We also include a new inductive bound for the minimum distance of generalized toric codes. As an application, we give new formulas for the minimum distance of generalized toric codes for special lattice point configurations.

2010 MSC: 14M25, 14G50, 52B20

Keywords: Toric code, Lattice polytope, Minkowski length, Sparse polynomials

1. Introduction

Toric codes are examples of a large class of evaluation codes studied by Goppa, Tsfasman, Vlădut, and others, using methods of algebraic geometry [18]. Yet the construction is very explicit: Given a lattice polytope P in $\mathbb{R}^m$, consider the set of all m-variate polynomials whose exponent vectors lie in P. The code is produced by evaluating these polynomials at the points of $(\mathbb{F}_q^*)^m$. This makes toric codes a wonderful example of an interconnection between algebraic geometry (toric varieties), geometric combinatorics (lattice polytopes), and coding theory. Toric codes were first introduced by J. Hansen in [7] for $m = 2$ and have been actively studied in the last decade. Here is a list of some recent papers on the subject: [8–11, 14, 16, 17, 19]. Apart from numerous theoretical results, about a dozen new "champion" toric codes and generalized toric codes have been found just recently [3, 4, 12]. A "champion" code is the one that has the largest known minimum distance for a given block length and dimension, as in the table of best known codes [6].

In this paper we concentrate on combinatorial questions about lattice polytopes which arise when one studies the minimum distance of toric codes. In Section 3 we relate the minimum distance to a geometric invariant called the Minkowski length of P. In particular, we look at the problem of estimating the number of lattice points in polytopes of fixed Minkowski length. The results there are not new, although some of them have not been published previously. Section 4 is concerned with generalized toric codes. There we prove a general inductive bound for the minimum distance. As an application we generalize previously known formulas for the minimum distance (Theorem 3.2) to generalized toric codes as well as provide some examples.

* *E-mail: i.soprunov@csuohio.edu*
The author is partially supported by NSA Grant H98230-13-1-0279

2. Preliminaries

2.1. Linear codes

To set our notation we start with basic definitions from coding theory. Throughout the paper, $\mathbb{F}_q$ denotes a finite field of q elements and $\mathbb{F}_q^*$ its multiplicative group of non-zero elements. A subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ is called a *linear code*, and its elements $c = (c_1, \ldots, c_n)$ are called *codewords*. The number n is called the *block length* of $\mathcal{C}$. The *weight* of c in $\mathcal{C}$ is the number of non-zero entries in c. The *distance* between two codewords a and b in $\mathcal{C}$ is the weight of $a - b \in \mathcal{C}$. The block length n, the dimension $k = \dim(\mathcal{C})$, and the minimum distance $d = d(\mathcal{C})$ are the parameters of $\mathcal{C}$. A code with parameters n, k, and d is referred to as an $[n, k, d]_q$-code.

2.2. Newton polytopes

Let f be a polynomial in m variables over a field $\mathbb{K}$. If we allow negative exponents in the monomials of f we call it a Laurent polynomial. The set of the exponent vectors of the monomials appearing in f is called the *support* of f, denoted by $\mathcal{A}(f)$. Thus we may write

$$f = \sum_{a \in \mathcal{A}(f)} c_a t^a, \text{ where } t^a = t_1^{a_1} \cdots t_m^{a_m}, \ c_a \in \mathbb{K}.$$

The *Newton polytope* $P(f)$ is the convex hull of the support of f. It is a convex lattice polytope in $\mathbb{R}^m$. (A polytope is called *lattice* if its vertices lie in $\mathbb{Z}^m \subset \mathbb{R}^m$.) For example, the Newton polytope of $f(t_1, t_2) = t_1^{-1} + 2t_1^{-1}t_2 - 3t_1t_2$ is the triangle with vertices $(-1, 0)$, $(-1, 1)$ and $(1, 1)$.

Notice that it makes sense to evaluate Laurent polynomials at points none of whose coordinate is zero, i.e., points in the algebraic torus $\mathbb{T}^m = (\mathbb{K}^*)^m$. Laurent polynomials with a prescribed Newton polytope are usually called *sparse polynomials* to emphasize that, compared to a generic polynomial of the same degree, it may have only a few monomials (the ones that correspond to the lattice points in its Newton polytope).

The Newton polytope plays the role of the degree for a sparse polynomial. Note that for any two sparse polynomials f, g we have $P(fg) = P(f) + P(g)$, just as for usual degrees. The sum here is the *Minkowski sum* of the polytopes, which is the set of all sums $p_1 + p_2$ for all pairs $p_1 \in P(f)$ and $p_2 \in P(g)$, and turns out to be again a polytope. Therefore, factorizations of a sparse polynomial are related to Minkowski sum decompositions of its Newton polytope. We will see in Section 3 how this relation helps to estimate the number of solutions to $f = 0$ over a finite field in terms of the Newton polytope $P(f)$.

Here is a bit of terminology. We say a lattice segment in $\mathbb{R}^m$ is *primitive* if it contains exactly two lattice points. We say a lattice simplex $\mathbb{R}^m$ is *unimodular* if it contains exactly $m + 1$ lattice points. We say a lattice triangle in $\mathbb{R}^2$ is *exceptional* if it contains exactly three boundary lattice points and one interior lattice point.

3. Toric codes

Let $\{p_1, \ldots, p_n\}$ be the set of all points in the algebraic torus $\mathbb{T}^m = (\mathbb{F}_q^*)^m$ in some linear order. Fix a lattice polytope $P \subset \mathbb{R}^m$ and let $\mathcal{L}(P)$ be the finite-dimensional space of Laurent polynomials over $\mathbb{F}_q$ whose support is contained in P:

$$\mathcal{L}(P) = span_{\mathbb{F}_q}\{t^a \mid a \in P \cap \mathbb{Z}^m\}. \tag{1}$$

We have the following *evaluation map*

$$ev_{\mathbb{T}^m} : \mathcal{L}(P) \to \mathbb{F}_q^n, \quad f \mapsto (f(p_1), \ldots, f(p_n)). \tag{2}$$

The image of $ev_{\mathbb{T}^m}$ is called the *toric code* and is denoted by $\mathcal{C}_P$.

Remark 3.1. *One may regard toric codes as a multivariate generalization of the Reed–Solomon codes. Indeed, if $m = 1$ and P is the lattice segment $[0, \ell]$ the toric code $\mathcal{C}_P$ coincides with the Reed–Solomon code with parameters $[q-1, \ell+1, q-1-\ell]_q$.*

Clearly, the block length n of $\mathcal{C}_P$ equals $(q-1)^m$, the size of $\mathbb{T}^m$. In [14] D. Ruano showed that the dimension k of $\mathcal{C}_P$ equals the number of lattice points of P if no two of them are congruent modulo $(\mathbb{Z}_{q-1})^m$. In particular, this is true if we assume that P is contained in the cube $K_q^m = [0, q-2]^m$. The main problem we are concerned with is how to compute or estimate the minimum distance $d = d(\mathcal{C}_P)$.

We will start with some explicit results. J. Little and R. Schwarz in [11] computed the minimum distance of $\mathcal{C}_P$ in the case of $P = \ell\Delta_m$, the standard m-simplex of side length ℓ and $P = \Pi_{\ell_1,\dots,\ell_m}$, the product of m segments $[0, \ell_1] \times \cdots \times [0, \ell_m]$:

$$d(\mathcal{C}_{\ell\Delta_m}) = (q-1)^{m-1}(q-1-\ell), \quad d(\mathcal{C}_{\Pi_{\ell_1,\dots,\ell_m}}) = \prod_{i=1}^{m}(q-1-\ell_i).$$

It turned out that this is an instance of a general phenomenon. In the following theorem we describe how the minimum distance behaves under basic operations on lattice polytopes (see [17] for details).

Theorem 3.2. *[17]*

1. *Let $P \subseteq K_q^{m_1}$ and $Q \subseteq K_q^{m_2}$ be lattice polytopes. Then*
$$d(\mathcal{C}_{P\times Q}) = d(\mathcal{C}_P)\, d(\mathcal{C}_Q).$$
2. *Let Q be a lattice polytope of $\dim Q \geq 1$, and let $\{kQ \mid 0 \leq k \leq N\}$ be a sequence of k-dilates of Q, contained in K_q^m. Let $\mathcal{P}(Q)$ be the pyramid over Q, i.e. the convex hull in $\mathbb{R}^{m+1}$ of the set $\{(x, 0) \mid x \in Q\} \cup \{e_{m+1}\}$. Then*
$$d(\mathcal{C}_{k\mathcal{P}(Q)}) = (q-1)\, d(\mathcal{C}_{kQ}).$$

Using this result one can compute the minimum distance explicitly for a large class of polytopes obtained from a lattice segment by taking the direct product or constructing a pyramid and dilating. In particular, Umana and Velasco [19] used this to compute the minimum distance for toric codes on *degree one* polytopes. In Section 4 we generalize this theorem to generalized toric codes.

Next we turn to the case of arbitrary polytopes. The situation is far from being understood even in the case of polytopes of small dimension. The first results in this direction were obtained by Hansen [7, 8] who used intersection theory on the toric surface defined by the lattice polygon to obtain lower bound for the minimum distance of $\mathcal{C}_P$. It turns out that there is a more direct relation between $d(\mathcal{C}_P)$ and geometry of lattice polytopes (at least for large q) — the minimum distance $d(\mathcal{C}_P)$ can be bounded in terms of what is called the Minkowski length of P. Here is the definition.

Definition 3.3. *Let P be a lattice polytope in $\mathbb{R}^m$. The Minkowski length of P is the maximum number of lattice polytopes of positive dimension whose Minkowski sum is contained in P:*

$$L(P) = \max\{\ell \,|\, Q_1 + \cdots + Q_\ell \subseteq P, \dim Q_i > 0\}.$$

A Minkowski decomposition of Q into $L(P)$ summands of positive dimension will be referred to as a maximal decomposition in P and Q will be called maximal.

It is not hard to see that there are only finitely many lattice polytopes Q contained in P and there are only finitely many possible decompositions of Q into the Minkowski sum of lattice polytopes of positive dimension, so the number $L(P)$ is well-defined. Moreover, it is easy to see that in the definition of $L(P)$ one may assume that the Q_i are lattice segments.

Recall from Section 2 that a factorization of a sparse polynomial corresponds to Minkowski sum decomposition of its Newton polytope. Therefore, the Minkowski length is the geometric invariant of P which describes the largest possible number of factors in factorizations of polynomials $f \in \mathcal{L}(P)$.

Consider the case $m = 2$. One can use the Hasse–Weil bound to estimate the number of zeroes in $\mathbb{T}^2$ of absolutely irreducible factors of $f \in \mathcal{L}(P)$. Little and Schenck in [10] used this bound to show that the more factors f has, the more it has zeroes in $\mathbb{T}^2$, provided q is large enough. It turns out that if $f \in \mathcal{L}(P)$ has a factorization with the largest number of factors then the Newton polytope of each factor is either a primitive segment, or a unimodular triangle, or an exceptional triangle, see [16]. Moreover, we have the following lower bound for the minimum distance of $\mathcal{C}_P$.

Theorem 3.4. *[16] Let P be a lattice polygon of Minkowski length L. There is an explicit function $\alpha(P)$ such that for all $q \geq \alpha(P)$ we have*

$$d(\mathcal{C}_P) \geq (q-1)(q-1-L) - (2\sqrt{q}-1).$$

Moreover, the term $2\sqrt{q}-1$ may be omitted if no maximal decomposition of P contains an exceptional triangle.

There is a natural action of the isomorphism group $AGL(m,\mathbb{Z})$ of the lattice $\mathbb{Z}^m$ on the space of lattice polytopes, under which $L(P)$ is invariant. The group $AGL(m,\mathbb{Z})$ consists of translations by a lattice vector and integer linear non-degenerate transformations, called unimodular transformations. Let P and P' be $AGL(m,\mathbb{Z})$-equivalent. Then the corresponding toric codes $\mathcal{C}_P$ and $\mathcal{C}_{P'}$ are monomially equivalent [11] (although the opposite is not true, see [13] for a counterexample). This means that for the purpose of coding theory it is enough to consider lattice polytopes up to $AGL(m,\mathbb{Z})$-equivalence.

Returning to Definition 3.3, note that each summand in a maximal decomposition has $L(Q_i) = 1$. Such polytopes are called *strongly indecomposable* and they play an important role in estimating the minimum distance $d(\mathcal{C}_P)$, see [16], as well as [20, Chapter 2].

In dimension $m = 2$ there are exactly three strongly indecomposable polytopes up to $AGL(m,\mathbb{Z})$-equivalence: the unit segment, the unit triangle, and the exceptional triangle, see Figure 1.

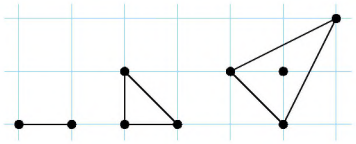

Figure 1. Strongly indecomposable polytopes up to $AGL(2,\mathbb{Z})$-equivalence.

Note that the latter has the largest number of lattice points, which is four. The following theorem is a generalization of this fact, which was discovered by I. Barnett, B. Fulan, C. Quinn, and J. Soprunova in an REU project at Kent State University in 2011. Since this result is not written up anywhere we include a short proof here.

Theorem 3.5. *Let $Q \subset \mathbb{R}^m$ be strongly indecomposable. Then the number of lattice points in Q is at most 2^m. Moreover, there exist strongly indecomposable polytopes with exactly 2^m lattice points.*

Proof. For the first part, consider the lattice points of Q modulo $(\mathbb{Z}/2\mathbb{Z})^m$. If Q has more than 2^m lattice points then there exists distinct lattice points $a, b \in Q \cap \mathbb{Z}^m$ which coincide modulo $(\mathbb{Z}/2\mathbb{Z})^m$. Then the lattice segment $[a,b] \subset Q$ must contain at least one interior lattice point, hence, decomposes into lattice segments. This contradicts the assumption that $L(Q) = 1$.

The construction of Q for which the bound is attained is by induction on m. We start with the exceptional triangle in $\mathbb{R}^2$. After a unimodular transformation we may assume that it contains no horizontal lattice segments, i.e. segments whose direction vector has zero first coordinate. We will call the direction vector of a lattice segment in a polytope P simply a *direction vector in P*.

Assume that $P \subset \mathbb{R}^m$ is a strongly indecomposable polytope with 2^m lattice points, such that no direction vector in P has zero first coordinate. Let k be the largest first coordinate of all direction vectors in P. There is a unimodular transformation $\alpha \in GL(m, \mathbb{Z})$ such that every direction vector in $\alpha(P)$ has the first coordinate greater than k. For example, we can take $\alpha = \alpha_2 \oplus id_{m-2}$, where α_2 has matrix $\begin{bmatrix} a & 1 \\ a-1 & 1 \end{bmatrix}$ with large enough a.

Finally, let P' be the convex hull of $P \times \{0\} \cup \alpha(P) \times \{1\}$ in $\mathbb{R}^{m+1}$. To show that P' is strongly indecomposable it is enough to show that there are no lattice segments of length more than one connecting a point in P and a point in $\alpha(P)$, and there are no lattice parallelograms with two vertices in P and two vertices in $\alpha(P)$. The former is clear since all lattice points in P' are distinct modulo $(\mathbb{Z}/2\mathbb{Z})^{m+1}$. The latter follows from the fact that the first coordinate of every direction vector in $\alpha(P)$ is greater than the first coordinate of any direction vector in P. □

There has been recent progress in understanding the structure of polytopes with $L(P) = 1$ in higher dimensions. In particular, new results have been obtained about 3-dimensional lattice polytopes and longest Minkowski sum decompositions of their subpolytopes [1]. As for the bounds in Theorem 3.4, a similar approach was taken in [20] for 3-dimensional toric codes. The author gives an algorithmic way of obtaining lower bound for the minimum distance, but one still hopes for more explicit bounds than the ones in [20].

Classifying polytopes of Minkowski length larger than one is not easy even in dimension $m = 2$. In Figure 2 we present 16 classes of lattice polygons of Minkowski length two. The proof that these are all of them is not hard, but tedious, so we do not include it here.

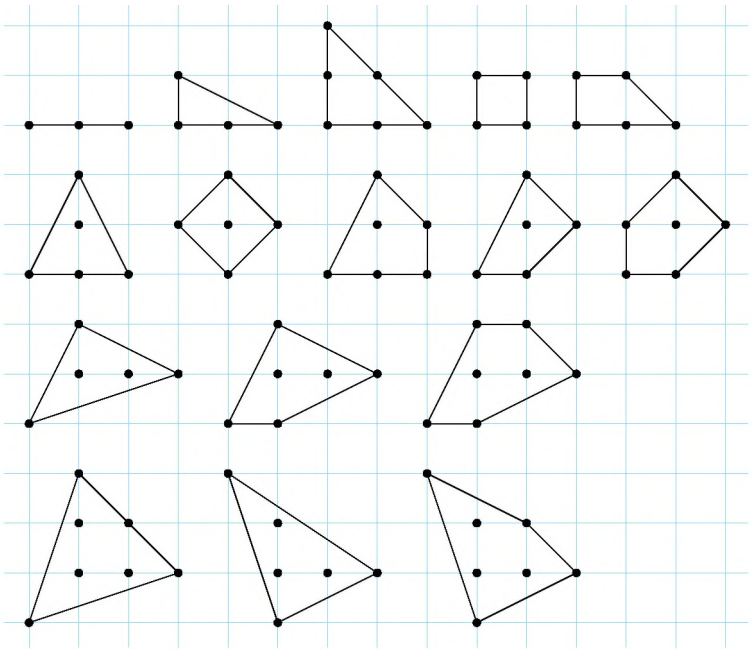

Figure 2. The sixteen polytopes with $L(P) = 2$ up to $GL(2, \mathbb{Z})$-equivalence.

It does not seem feasible to classify polygons with $L(P) \geq 3$ by hand. Recall that the dimension of a toric code equals the number of lattice points in P. Thus, a more important question is the following: Given ℓ, what could be the largest number of lattice points in P with $L(P) = \ell$? The naive bound $|P \cap \mathbb{Z}^m| \leq (\ell + 1)^m$ which follows from considering the lattice points of P modulo $(\mathbb{Z}/(\ell + 1)\mathbb{Z})^m$, as in the proof of Theorem 3.5, appears to be too rough.

Suppose $m = 2$, so P is a lattice polygon. From Figure 2 we see that for $\ell = 2$ the answer is 7. In [5] V. Cestaro showed that for $\ell = 3$ the answer is 9. For larger ℓ the question is open and no better estimate than $(\ell + 1)^2$ is currently known.

4. Generalized Toric codes

Generalized toric codes are a natural extension of toric codes. They first appeared in the work of D. Ruano [15] and J. Little [12]. The definition is similar to the one of a toric code, except we allow arbitrary configurations of lattice points instead of the lattice points of a lattice polytope. More precisely, let S be a set of lattice points in $\mathbb{R}^m$ contained in the m-cube K_q^m. Similar to (1) we let $\mathcal{L}(S)$ be the vector space over $\mathbb{F}_q$ of Laurent polynomials with support in S:

$$\mathcal{L}(S) = span_{\mathbb{F}_q}\{t^a \mid a \in S\}.$$

The image of the corresponding evaluation map

$$ev_{\mathbb{T}^m} : \mathcal{L}(S) \to \mathbb{F}_q^n, \quad f \mapsto (f(p_1), \ldots, f(p_n)).$$

is called the *generalized toric code* $\mathcal{C}_S$. The weight of each nonzero codeword equals the number of points $\xi \in \mathbb{T}^m$ where the corresponding polynomial does not vanish. We denote it by $w(f)$. Let $Z(f)$ denote the number of zeroes of f in $\mathbb{T}^m$. Also let Z_S denote the maximum number of zeroes over all nonzero $f \in \mathcal{L}(S)$. Obviously,

$$Z(f) = (q-1)^m - w(f) \quad \text{and} \quad Z_S = (q-1)^m - d(S). \tag{3}$$

As before, $\mathcal{C}_S$ is a linear code of block length $n = (q-1)^m$ and dimension $\dim \mathcal{C}_s = |S|$, the cardinality of S. Note that if P is the convex hull of S then

$$\dim \mathcal{C}_S \le \dim \mathcal{C}_P \quad \text{and} \quad d(\mathcal{C}_S) \ge d(\mathcal{C}_P).$$

The idea is that by omitting just a few lattice points of P one could, in principle, obtain S for which the minimum distance $d(\mathcal{C}_S)$ is significantly larger than $d(\mathcal{C}_P)$. Examples of this phenomenon were provided by J. Little [12]. At the same time he gave some evidence that for large q this often does not happen.

This prompted a search for generalized toric codes with parameters better than previously known over fields of small size. G. Brown and A. Kasprzyk [3, 4] used an exhaustive search of lattice polygons and lattice point configurations contained in K_q^2 for q up to 8. They were able to find a new toric code champion and seven new generalized toric code champions.

4.1. Two examples

Below we give two examples of generalized toric code with best known parameters. The corresponding configurations (see Figure 3) are $AGL(2,\mathbb{Z})$-equivalent to the ones found in [4]. They produce a $[49, 13, 27]$-code and a $[49, 19, 21]$-code over $\mathbb{F}_8$, respectively.

As pointed out by Markus Grassl (private communication), by omitting the point $(1, 2)$ in S one obtains a subcode with parameters $[49, 12, 28]$. Applying Construction X to this pair of codes (see [6]), one obtains a $[50, 13, 28]$-code over $\mathbb{F}_8$, which gave another champion.

4.2. Inductive bound

We finish with a new general lower bound for the minimum distance of generalized toric codes. The bound is inductive in a sense that it uses the codes from the fibers and the images of a projection of S

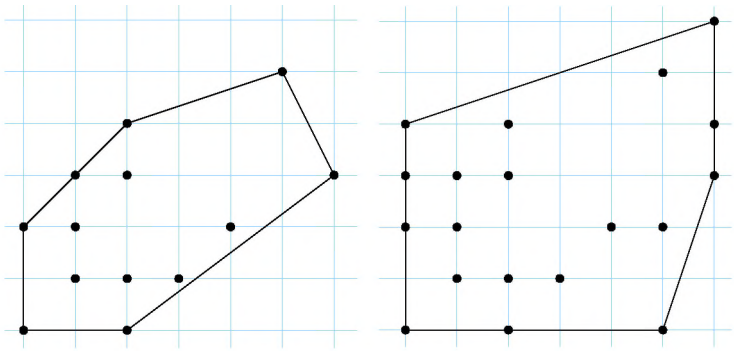

Figure 3. Two lattice configurations producing a $[49, 13, 27]$- and $[49, 19, 21]$-code over $\mathbb{F}_8$.

onto a coordinate subspace. As a corollary we get a generalization of Theorem 3.2 to generalized toric codes.

Let $S \subseteq K_q^m$ be a set of lattice points. Choose a coordinate subspace $Y \subseteq \mathbb{R}^m$ (defined by setting a subset of coordinates equal zero) and let $\pi : \mathbb{R}^m \to Y$ be the corresponding projection. For every $a \in \pi(S)$ let S_a denote the fiber $S_a = S \cap \pi^{-1}(a)$.

Theorem 4.1. *Let S be a set of lattice points in K_q^m and $\pi : \mathbb{R}^m \to Y$ a projection onto a coordinate subspace. Then*

$$d(S) \geq \min_{S' \subseteq \pi(S)} \left(d(S') \max_{a \in S'} d(S_a) \right).$$

Proof. We may assume that $\pi : \mathbb{R}^m \to Y$ is the projection onto the last $m-k$ coordinates. Furthermore, we use $(x, y) = (x_1, \ldots, x_k, y_1, \ldots, y_{m-k})$ to denote coordinates in $\mathbb{T}^m = \mathbb{T}^k \times \mathbb{T}^{m-k}$.

Consider an arbitrary nonzero $f \in \mathcal{L}(S)$ with support $\mathcal{A}(f)$, and let S' denote the projection $S' = \pi(\mathcal{A}(f))$. We have $\mathcal{A}(f) \subseteq \cup_{a \in S'} S_a$, hence, we can write f as a linear combination of monomials y^a for $a \in S'$ with coefficients f_a that are nonzero polynomials in $\mathcal{L}(S_a)$:

$$f(x, y) = \sum_{a \in S'} f_a(x) y^a. \tag{4}$$

Given a point $\xi = (\xi_1, \ldots, \xi_k) \in (\mathbb{F}_q^*)^k$ let L_ξ be the coset of the subtorus $\{\mathbf{1}\} \times (\mathbb{F}_q^*)^{m-k}$ containing ξ, i.e.

$$L_\xi = \{(\xi, y) \mid y \in (\mathbb{F}_q^*)^{m-k}\}.$$

Here $\mathbf{1}$ denotes the identity element in $(\mathbb{F}_q^*)^k$.

Note that on every L_ξ where f is identically zero, f has exactly $(q-1)^{m-k}$ zeroes, and on every L_ξ where f is not identically zero, it has at most $Z_{S'}$ zeroes, since the (nonzero) polynomial $f(\xi, y)$ lies in $\mathcal{L}(S')$.

Then the number of zeroes of f in $\mathbb{T}^m$ is bounded by

$$Z(f) \leq (q-1)^{m-k} N + Z_{S'} \left((q-1)^k - N \right), \tag{5}$$

where N is the number of the cosets L_ξ where f is identically zero. Substituting $Z_{S'} = (q-1)^{m-k} - d(S')$ (see (3)) and simplifying we obtain

$$Z(f) \leq (q-1)^m - d(S') \left((q-1)^k - N \right),$$

or, simply,

$$w(f) \geq d(S')\left((q-1)^k - N\right). \tag{6}$$

Notice that N is, in fact, the number of common zeroes of the f_a in $(\mathbb{F}_q^*)^k$, and is at most the number of zeroes of each f_a. Therefore,

$$N \leq \min_{a\in S'} Z(f_a) \leq (q-1)^k - \max_{a\in S'} d(S_a).$$

Now (6) implies

$$w(f) \geq d(S') \max_{a\in S'} d(S_a).$$

Notice that the right hand side depends only on the projection of the support of f, so it remains to take the minimum over all subsets $S' \subseteq \pi(S)$ and the statement of the theorem follows. □

Our first application of the inductive formula is a generalization of Theorem 3.2, part (1).

Corollary 4.2. *Suppose $S = S_1 \times S_2 \subset \mathbb{R}^{m_1} \times \mathbb{R}^{m_2}$ for some lattice sets $S_i \subseteq K_q^{m_i} \cap \mathbb{Z}^{m_i}$, $i = 1, 2$. Then $d(S) = d(S_1)d(S_2)$.*

Proof. Consider the projection $\pi : \mathbb{R}^{m_1} \times \mathbb{R}^{m_2} \to \mathbb{R}^{m_2}$. Then $\pi(S) = S_2$. As every fiber S_a equals a lattice translate of S_1, for $a \in S_2$, by Theorem 4.1 we have

$$d(S) \geq \min_{S'\subseteq S_2} (d(S')d(S_1)) = d(S_1) \min_{S'\subseteq S_2} d(S').$$

It is clear that if $S' \subseteq S_2$ then $d(S') \geq d(S_2)$. Therefore, the above minimum equals $d(S_2)$.

Conversely, let $f_i \in \mathcal{L}(S_i)$ for $i = 1, 2$ be polynomials with the minimum weight. We have $d(S_i) = w(f_i) = (q-1)^{m_i} - Z(f_i)$, where $Z(f_i)$ is the number of zeroes of f_i in $\mathbb{T}^{m_i}$. Then, by the inclusion-exclusion principle, the polynomial $f = f_1 f_2$ has

$$(q-1)^{m_2} Z(f_1) + (q-1)^{m_1} Z(f_2) - Z(f_1)Z(f_2)$$

zeroes in $\mathbb{T}^{m_1} \times \mathbb{T}^{m_2}$. This implies that its weight equals

$$w(f) = (q-1)^{m_1+m_2} - (q-1)^{m_2} Z(f_1) - (q-1)^{m_1} Z(f_2) + Z(f_1)Z(f_2) = w(f_1)w(f_2).$$

Therefore, $d(S) \leq d(S_1)d(S_2)$, and we are done. □

Corollary 4.3. *Let $\pi_m : \mathbb{R}^m \to \mathbb{R}$ be the projection to the last coordinate and suppose $\pi_m(S) = \{0, 1, \ldots, \ell\}$. If $d(S_0) \leq d(S_1) \leq \cdots \leq d(S_\ell)$ then*

$$d(S) \geq \min_{0\leq i\leq \ell} (q-1-i)d(S_i).$$

Proof. Indeed, consider $S' \subset \pi_m(S)$ and let i be the length of the convex hull of S'. On one hand we have $d(S') \geq (q-1-i)$. On the other hand, since $d(S_0) \leq d(S_1) \leq \cdots \leq d(S_\ell)$, when finding the minimum over all S' it is enough to consider only those S' that contain 0. In that case $\max_{a\in S'} d(S_a) = d(S_i)$ and the statement follows from Theorem 4.1. □

To connect this result to the second part of Theorem 3.2, we will need an extra assumption on the configuration S. First, we have the following proposition. Its proof is similar to the one of [17, Proposition 2.2]

Proposition 4.4. *Let S, S' be lattice sets in K_q^m and T the set of lattice points of a lattice segment. If $S + T \subseteq S'$ (up to a lattice translation) then $(q-1)d(S') \leq (q - |T|)d(S)$.*

Proof. After a unimodular transformation we may assume that $S+T \subseteq S'$, and T is the set of lattice points of the segment $[0, ke_1]$, where e_1 is the first basis vector and $k = |T| - 1$ is the length of the segment.

Let $g \in \mathcal{L}(S)$ be a polynomial with $Z(g) = Z_S$. Then for any $\xi_1, \dots, \xi_k \in \mathbb{F}_q^*$ the polynomial

$$f(x) = g(x) \prod_{j=1}^{k} (x_1 - \xi_j)$$

belongs to $\mathcal{L}(S+T) \subseteq \mathcal{L}(S')$. By the inclusion-exclusion formula we have

$$Z(f) = Z(g) + k(q-1)^{m-1} - \sum_{j=1}^{k} Z(g|_{x_1=\xi_j}).$$

Since $\mathbb{T}^m$ is the union of $q-1$ subtori given by $x_1 = \xi$, for $\xi \in \mathbb{F}_q^*$, we have $Z(g) = \sum_{\xi \in \mathbb{F}_q^*} Z(g|_{x_1=\xi})$. Choose $\xi_1, \dots, \xi_k \in \mathbb{F}_q^*$ so that $\{Z(g|_{x_1=\xi_j}) \mid j = 1, \dots, k\}$ are the k smallest integers among the $q-1$ integers $\{Z(g|_{x_1=\xi}) \mid \xi \in \mathbb{F}_q^*\}$. Then

$$\frac{1}{k} \sum_{j=1}^{k} Z(g|_{x_1=\xi_j}) \leq \frac{Z(g)}{q-1}.$$

Therefore, we obtain

$$Z_{S'} \geq Z(f) \geq Z(g) + k(q-1)^{m-1} - \frac{k}{q-1} Z(g)$$

Replacing $Z(g)$ with Z_S and using $Z_S = (q-1)^m - d(S)$ we see that the latter inequality is equivalent to $(q-1)d(S') \leq (q-k-1)d(S)$, as required. □

The following is a generalization of Theorem 3.2, part (2) to generalized toric codes.

Theorem 4.5. *Let S be a lattice set in $\mathbb{K}_q^m$. Let $\pi_m : \mathbb{R}^m \to \mathbb{R}$ be the projection to the last coordinate, $\pi_m(S) = \{0, 1, \dots, \ell\}$, and $S_0, \dots, S_\ell$ the corresponding fibers. Suppose there is a primitive lattice segment $[a, b]$ such that for every $1 \leq i \leq \ell$, the set $S_i + \{a, b\}$ is contained in S_{i-1}, up to a lattice translation. Then*

$$d(S) = (q-1)d(S_0).$$

Proof. First, note that in this special situation, the conditions of Corollary 4.3 are satisfied. Indeed, by Proposition 4.4, $(q-1)d(S_{i-1}) \leq (q-2)d(S_i)$, so in particular, $d(S_{i-1}) \leq d(S_i)$.

Next, we have $S_i + i\{a, b\} \subseteq S_0$ up to a lattice translation. Here $i\{a, b\}$ (which is the Minkowski sum of $\{a, b\}$ with itself i times) is the set of lattice points of a lattice segment of length i. Thus, by Proposition 4.4,

$$(q-1)S_0 \leq (q-1-i)d(S_i),$$

for every $0 \leq i \leq \ell$. Applying Corollary 4.3, we obtain

$$d(S) \geq (q-1)d(S_0).$$

Conversely, let $g \in \mathcal{L}(S_0)$ be a polynomial with $Z(g) = Z_{S_0}$. By definition, g depends only on the first $m-1$ variables. Therefore, it has $(q-1)Z_{S_0}$ zeroes in $\mathbb{T}^m$. This implies that $Z_S \geq (q-1)Z_{S_0}$, i.e. $d(S) \leq (q-1)d(S_0)$. □

The last result can be applied to constructing a generalized toric code with parameters $[(q-1)n, k', (q-1)d]$ from a given generalized toric $[n,k,d]$-code. As an example, let S_0 be the 13-point configuration in Figure 3. For the primitive segment $[a,b]$ we choose $a=(0,0)$ and $b=(1,1)$. Then by removing the points with the largest sum of coordinates in every line parallel to $[a,b]$ we obtain a 6-point configuration S_1 satisfying $S_1+\{a,b\}\subset S_0$. A repetition of this process produces a 2-point configuration S_2 satisfying $S_2+\{a,b\}\subset S_1$. Now define $S=\bigcup_{i=0}^{2} S_i\times\{i\}$, which is a 21-point configuration in $\mathbb{Z}^3$. According to Theorem 4.5, the corresponding generalized toric code has parameters $[343,21,189]$ over $\mathbb{F}_8$.

Acknowledgment: The first part of this paper is based on a talk given at Karatekin Mathematics Days 2014 International Mathematics Symposium. I am grateful to the organizers for inviting me and to Mesut Şahin, Pinar Celebi Demirarslan, and Gökhan Demirarslan for their hospitality.

References

[1] O. Beckwith, M. Grimm, J. Soprunova, B. Weaver, *Minkowski length of 3D lattice polytopes*, Discrete and Computational Geometry 48, Issue 4, 1137-1158, 2012.
[2] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24, 235-265, 1997.
[3] G. Brown, A. M. Kasprzyk, *Small polygons and toric codes*, Journal of Symbolic Computation, 51, 55-62, April 2013.
[4] G. Brown, A. M. Kasprzyk, *Seven new champion linear codes*, LMS Journal of Computation and Mathematics, 16, 109-117, 2013.
[5] V. Cestaro, *Parameters of toric codes in small dimension*, Senior undergraduate project, CSU 2011.
[6] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, online, http://www.codetables.de/, accessed on October 1, 2013.
[7] J. Hansen, *Toric surfaces and error-correcting codes* in Coding Theory, Cryptography, and Related Areas, Springer, 132-142, 2000.
[8] J. Hansen, *Toric varieties Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput., 13, 289-300, 2002.
[9] D. Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput., 15, 63-79, 2004.
[10] J. Little, H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. 20, no. 4, (electronic) 999-1014, 2006.
[11] J. Little, R. Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput., 18(4), 349-367, 2007.
[12] J. Little, *Remarks on generalized toric codes*, Finite Fields and Their Applications, 24, 1-14, November 2013.
[13] X. Luo, S. S.-T. Yau, M. Zhang, H. Zuo, *On classification of toric surface codes of low dimension*, arXiv:1402.0060.
[14] D. Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields and Their Applications, 13, 962-976, 2007.
[15] D. Ruano, *On the structure of generalized toric codes*, Journal of Symbolic Computation, 44(5), 499-506, 2009.
[16] I. Soprunov, J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math., 23(1), 384-400, 2009.
[17] I. Soprunov, J. Soprunova, *Bringing toric codes to the next dimension*, SIAM J. Discrete Math., 24(2), 655-665, 2010.
[18] M. Tsfasman, S. Vlădut, D. Nogin, *Algebraic geometric codes: Basic notions* Providence, R.I.: American Mathematical Society, 2007.
[19] V. G. Umana, M. Velasco *Dual toric codes and polytopes of degree one*, preprint arXiv:1404.4063.
[20] J. Whitney, *A bound on the minimum distance of three dimensional toric codes*, Ph.D. Thesis, 2010.